UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,215	01/26/2001	Robert H. Barron	2143.005	7357

21917 7590 06/25/2004

MCHALE & SLAVIN, P.A.
2855 PGA BLVD
PALM BEACH GARDENS, FL 33410

EXAMINER	
DENNISON, JERRY B	
ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 06/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/771,215	**Applicant(s)** BARRON, ROBERT H.
	Examiner J. Bret Dennison	**Art Unit** 2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to Application Number 09/771215 received on 26 January 2001.

2. Claims 1-37 and 40 are presented for examination.

Double Patenting (Obviousness)

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-6, 15 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6 of U.S. Patent No. 6,665,709. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows:

U.S. Patent No. 6,665,709	***Instant Application: 09/771215***
1. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:	***1.*** *A method of transporting electronic data for secure storage on an archive server, comprising the steps of:*
accessing a conventional web browser from a client computer; logging onto a qualified server and providing account qualifier data;	*providing at least one client workstation having a Web browser running thereon;* *accessing the Web browser from the client workstation and logging onto a qualitied Web server;* *providing account qualifier data to a software application residing on the Web server*
obtaining a first applet compiled on said server in response to the inquiry page, the first applet operable to perform the steps of	*obtaining an encryption applet from the software application;*
allowing a client to select a data file to be transferred to the qualified server,	*selecting an electronic data file to be encrypted;*
generating a unique random encryption sequence, encrypting the selected data file to form an encrypted data packet;	*encrypting said electronic data file and forming an encrypted data packet;*
forwarding the data packet to said qualified	*transferring said encrypted data packet to*

server for storage; storing the randomly generated encryption sequence on the qualified server; and	*the archive server; and*
deleting the first applet from the client computer;	*destroying the encryption applet.*
2. The method of claim 1, wherein the software application residing on the Web server is platform-independent.	***2.*** *The method of claim 1, wherein the software application residing on the Web server is platform-independent.*
3. The method of claim 1, further including the step of compressing the encrypted data packet prior to transferring the encrypted data packet to the archive server.	***3.*** *The method of claim 1, further including the step of compressing the encrypted data packet prior to transferring the encrypted data packet to the archive server.*
4. The method of claim 3, wherein the encryption applet includes a compression program to compress the electronic data to form a compressed encrypted data packet.	***4.*** *The method of claim 3, wherein the encryption applet includes a compression program to compress the electronic data to form a compressed encrypted data packet.*
5. The method of claim 1, wherein the encryption applet compiled by the software application is based on an encryption algorithm, and the encryption algorithm is	***5.*** *The method of claim 1, wherein the encryption applet compiled by the software application is based on an encryption algorithm, and the encryption algorithm is*

changeable with respect to the software application.	*changeable with respect to the software application.*
6. The method of claim 1, further comprising the steps of:	***6.*** *The method of claim 1, further comprising the steps of:*
providing a plurality of encryption algorithms;	*providing a plurality of encryption algorithms;*
selecting an encryption algorithm; and	*selecting an encryption algorithm; and*
compiling the encryption applet using the selected encryption algorithm.	*compiling the encryption applet using the selected encryption algorithm.*
1. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:	**15.** A method of retrieving encrypted electronic data stored on an archive server, comprising the steps of:
providing a means for decrypting said encrypted data packet comprising the steps of:	providing at least one encrypted data packet on the archive server;
accessing a conventional web browser; logging onto a qualified server and providing account qualifier data;	providing at least one client workstation having a Web browser; accessing the Web browser and logging onto a qualified Web server; providing account qualifier data to a software application residing on the Web
allowing the recipient to select a file to be	selecting an encrypted data packet to be

retrieved from the qualified server;	retrieved from the archive server;
obtaining a second applet compiled on the server in response to said inquiry page, the second applet operable to perform the steps of displaying files available to a recipient; calculating the decryption sequence based on the original encryption sequence;	obtaining a decryption applet from the application based on the original encryption algorithm of the encrypted data packet;
retrieving the encrypted data packet and original encryption sequence associated with the selected file;	transferring the decryption applet and the encrypted data packet to the client workstation; and
decrypting the encrypted data packet;	decrypting said encrypted data packet at the client workstation, whereby the electronic data is available to a user at the client workstation.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Claim Objections

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

3. Misnumbered claim 40 has been renumbered 38.

4. Claim 15 is objected to because of the following informalities: Claim 15 recites the limitation, "providing account qualifier data to as software..." on line 6 of the claim, page 20. The limitation will be interpreted as, "providing account qualifier data to a software ..." Appropriate correction is required.

5. Claim 24 is objected to because of the following informalities: Claim 24 recites the limitation "wherein the encrypted data packet is transferred from the to the archive server..." on line 5 of the claim, page 22. The limitation will be interpreted as "wherein the encrypted data packet is transferred from the archive server ..." Appropriate correction is required.

6. Claim 25 is objected to because of the following informalities: Claim 25 recites the limitation "means for qualifying a authorization..." on line 5 of the claim, page 22. The limitation will be interpreted as a "means for qualifying an authorization..." Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 2 are rejected under 35 U.S.C. 102(e) as being anticipated by Holloway (U.S. Patent Number 6,424,718).

7. Regarding claim 1, Holloway discloses a method of transporting electronic data for secure storage on an archive server, comprising the steps of:

providing at least one client workstation having a Web browser running thereon (Holloway, col. 5, lines 14-15);

accessing the Web browser from the client workstation and logging onto a qualified Web server and providing account qualifier data to a software application residing on the Web server (Holloway, col. 7, last paragraph);

obtaining an encryption applet from the software application (Holloway, col. 7, lines 50-57);

selecting an electronic data file to be encrypted (Holloway, col. 8, lines 18-22);

encrypting said electronic data file and forming an encrypted data packet (Holloway, col. 8, lines 22-24) transferring said encrypted data packet to the archive server (Holloway, col. 8, lines 31-35; and

destroying the encryption applet (Holloway, col. 7, lines 48-61).

8. Regarding claim 2, Holloway teaches the limitations, substantially as claimed, as described in claim 1, including wherein the software application residing on the Web server is platform-independent (Holloway, col. 5, lines 50-60).

9. Regarding claim 5, Holloway teaches the limitations, substantially as claimed, as described in claim 1, including wherein the encryption applet compiled by the software application is based on an encryption algorithm, and the encryption algorithm is changeable with respect to the software application (Holloway, col. 7, line 60 through col. 8, line 10, Holloway teaches using any conventional cryptographic techniques).

10. Regarding claim 8, Holloway teaches the limitations, substantially as claimed, as described in claim 1, including providing a plurality of client workstations, wherein at least two of the plurality of client workstations are coupled via a network (Holloway, col. 3, lines 30-40).

11. Regarding claim 9, Holloway teaches the limitations, substantially as claimed, as described in claim 8, including wherein the archive server is coupled to at least one of the plurality of client workstations (Holloway, col. 3, lines 30-40).

12. Regarding claim 10, Holloway teaches the limitations, substantially as claimed, as described in claim 8, including wherein the archive server is coupled to the network (Holloway, col. 3, lines 40-44).

13. Regarding claim 11, Holloway teaches the limitations, substantially as claimed, as described in claim 1, including the step of assigning access permission to said encrypted data packet, wherein the access permission permits selective access to the electronic data files (Holloway, col. 8, lines 20-25).

14. Regarding claim 12, Holloway teaches the limitations, substantially as claimed, as described in claim 11, including wherein access permission is assigned to a user having designated account qualifier data (Holloway, col. 7, lines 60-67).

15. Regarding claim 14, Holloway teaches the limitations, substantially as claimed, as described in claim 1, including wherein the encrypted data packet is transferred from the client workstation to the archive server by SSL protocol.

16. Regarding claim 15, Holloway discloses a method of retrieving encrypted electronic data stored on an archive server, comprising the steps of:

providing at least one encrypted data packet on the archive server (Holloway, col. 7, lines 50-57);

providing at least one client workstation having a Web browser (Holloway, col. 5, lines 14-15);

accessing the Web browser and logging onto a qualified Web server (Holloway, col. 7, last paragraph);

providing account qualifier data to as software application residing on the Web server (Holloway, col. 7, last paragraph);

selecting an encrypted data packet to be retrieved from the archive server (Holloway, col. 9, lines 12-24);

obtaining a decryption applet from the application based on the original encryption algorithm of the encrypted data packet (Holloway, col. 9, lines 12-24);

transferring the decryption applet and the encrypted data packet to the client workstation (Holloway, col. 9, lines 12-24); and

decrypting said encrypted data packet at the client workstation, whereby the electronic data is available to a user at the client workstation (Holloway, col. 9, lines 24-46).

17. Regarding claim 16, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the account qualifier data corresponds to at least One user (Holloway, col. 7, last paragraph).

18. Regarding claim 18, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the software application residing on said Web server is platform-independent (Holloway, col. 5, lines 50-60).

19. Regarding claim 19, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the at least one client workstation comprises a plurality of client workstations (Holloway, col. 3, lines 30-40).

20. Regarding claim 20, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the at least two of the plurality of client workstations are coupled via a network (Holloway, col. 3, lines 30-40).

21. Regarding claim 21, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the archive server is coupled to the at least one client workstation (Holloway, col. 3, lines 30-40).

22. Regarding claim 22, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the archive server is coupled to the network (Holloway, col. 3, lines 40-44).

23. Regarding claim 23, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein access permission is assigned to at least

one encrypted data packet, wherein the access permission permits selective access to the electronic data files (Holloway, col. 9 , lines 10-25).

24. Regarding claim 24, Holloway teaches the limitations, substantially as claimed, as described in claim 15, including wherein the encrypted data packet is transferred from the archive server to the client workstation by SSL protocol (Holloway, col. 7, lines 65-67).

25. Regarding claim 25, Holloway discloses a system for secure storage of electronic data on an archive server, comprising:

a plurality of client workstations, said plurality of client workstations having Web browsers running thereon (Holloway, col. 3, lines 30-40 and col. 5, lines 14-15);

a platform-independent software application residing on a Web server (Holloway, col. 6, lines 20-30);

means for qualifying an authorization user of said software application (Holloway, col. 7, last paragraph);

means for encrypting an electronic file at said client workstations, said means comprising an encryption applet compiled by said software application which is transmitted to a user at one of said client workstations (Holloway, col. 7, lines 53-57); said encryption applet operable to encrypt the electronic file to create an encrypted data packet (Holloway, col. 8, lines 22-34);

means for transmitting said encrypted data packet to said archive server for secure storage (Holloway, col. 8, lines 31-35);

means for retrieving said encrypted data packet from said archive server (Holloway, col. 9, lines 12-24); and

means for decrypting said encrypted data packet, said means comprising obtaining a decryption applet from said software application, said decryption applet compiled by said software application based on the original encryption algorithm (Holloway, col. 9, lines 24-46).

26. Regarding claim 30, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein two of the plurality of client workstations are coupled via a network (Holloway, col. 3, lines 30-40).

27. Regarding claim 31, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein the archive server is coupled to at least one of the plurality of client workstations (Holloway, col. 3, lines 30-40).

28. Regarding claim 32, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein the archive server is coupled to the network (Holloway, col. 3, lines 40-44).

29. Regarding claim 33, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein access permission is assigned to said

encrypted data packet, wherein said access permission permits selective access to the electronic data files (Holloway, col. 9, lines 10-25).

30. Regarding claim 34, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein said access permission is assigned to a user having designated account qualifier data (Holloway, col. 7, last paragraph).

31. Regarding claim 36, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein the means for transmitted the encrypted data packet from the archive server is by SSL protocol (Holloway, col. 7, lines 65-67).

32. Regarding claim 38, Holloway teaches the limitations, substantially as claimed, as described in claim 25, including wherein said software application is accessed by account qualifier data (Holloway, col. 7, last paragraph).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 4, 13, 17, 26, 27, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holloway.

33. Regarding claims 3, 4, and 26, Holloway teaches the limitations, substantially as claimed, as described in claim 1. However, Holloway fails to teach the applet including a compression program to form a compressed encrypted data packet prior to transferring the encrypted data packet to the archive server.

It would have been obvious to one in the ordinary skill in the art at the time the invention was made to use a compression program for the purpose of reducing the amount of time for transfer of data to the server.

34. Regarding claims 17 and 27, Holloway teaches the limitations, substantially as claimed, as described in claim 15. However, Holloway fails to teach wherein said encrypted data packet is compressed, and said decryption applet includes a decompression program to decompress the encrypted data packet.

It would have been obvious to one in the ordinary skill in the art at the time the invention was made to use compression and decompression on the encrypted data packet for the purpose of reducing the amount of time for transfer of data to/from the server.

35. Regarding claims 13 and 35, Holloway teaches the limitations, substantially as claimed, as described in claims 11 and 33. Holloway also discloses wherein access permission permits selective access to the electronic data files (Holloway, col. 9, lines 10-25). Holloway does not explicitly state wherein said access permission permits hierarchal access to an electronic data file by a group of users. However, it would have

been obvious to one in the ordinary skill in the art at the time of the invention to incorporate hierarchal access to data because it is a form of access permission.

Claims 6, 7, 28, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holloway in view of Schreiber et al. (U.S. Patent Number 6,298,446).

36. Regarding claims 6, 7, 28, and 29, Holloway teaches the limitations, substantially as claimed, as described in claims 1 and 25. However, Holloway does not explicitly state wherein the software application compiles the encryption applet using an encryption algorithm, and the encryption algorithm is selected from a plurality of encryption algorithms. In an analogous art of networking, Schreiber discloses a method for protecting data over a distributed network wherein the web server regularly changes the encryption algorithm (Schreiber, col. 28, lines 60-64) to use in the applet (Schreiber, col. 7, lines 1-20). Therefore, it would have been obvious to one in the ordinary skill in the art at the time the invention was made to combine Holloway and Schreiber to provide a secure method of enabling messages to be processed by only authorized users.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Caldwell et al. (U.S. Patent Number 6,421,673) discloses a method for mapping applications and or attributed network environment.

Fieres et al. (U.S. Patent Number 5,841,870) discloses dynamic classes of service for an international cryptography framework.

Shambroom (U.S. Patent Number 6,198,824) discloses a system for providing secure remote command execution network.

Murphy et al. (U.S. Patent Number 6,226,744) discloses a method and apparatus for authenticating users on a network using a smart card.

Debry (U.S. Patent Number 6,314,521) discloses secure configuration of a digital certificate for a printer or other network device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to J. Bret Dennison whose telephone number is (703)305-8756. The examiner can normally be reached on M-F 8:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (703)308-5221. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

J. Bret Dennison
Patent Examiner
Art Unit 2143

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100